**Amendments to the Claims**

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

Claims 1 to 30 (canceled)

31. (new) A method of establishing a session key between a pair of correspondents in a data communication system, each of said correspondents sharing secret information (d), said method comprising the steps of:

a) one of said correspondents generating additional secret information (k) and deriving therefrom a session key;

b) said one of said correspondents transferring said additional secret information (k) to the other of said correspondents; and

c) said other of said correspondents using said secret information (d) and said additional secret information (k) to generate a session key.

32. (new) A method of claim 31 wherein said secret information (d) and said additional secret information (k) are combined at said one correspondent in a signature algorithm to provide a first signature component and said additional secret information is obtained by said other correspondent by utilizing said secret information on said first signature component.

33. (new) A method of claim 32 wherein said first signature component includes public information associated with said other correspondent and said other correspondent utilizes said public information to obtain said additional secret information.

34. (new) A method according to claim 33 wherein said secret information (d) and said public information ($Q_B$) are combined in said signature algorithm and such combination is precomputed and stored by said one correspondent.

35. (new) A method according to claim 34 wherein said combination is the product of said secret information and said public information.

36. (new) A method according to claim 32 wherein a second signature component is derived from said shared key.

37. (new) A method according to claim 36 wherein a portion of said shared key is utilized to provide said second signature component.

38. (new) A method according to claim 37 wherein said shared key represents the coordinates of a point on an elliptic curve and said portion is one of said coordinates.

39. (new) A method according to claim 37 wherein said portion is hashed by a secure hash function to provide said second signature component.

40. (new) A method according to claim 36 wherein said signature is verified by operating upon the session key obtained at said other correspondent to obtain a value corresponding to said second signature component and comparing such value with said second signature component.

41. (new) A method of establishing a session key between a first correspondent and a selected one of a plurality of second corespondents corrected to said first correspondent, said method comprising providing each of said second correspondents a respective secret information, storing each of said secret informations at said first correspondent to associate each of said stored secret informations with a respective correspondent, receiving from said selected one of said second correspondents a signature including a first component combining said secret information with additional secret information used by said selected one of said second correspondents to generate a session key, retrieving said stored secret information associated with said selected one of said second correspondents and using said secret information and said additional secret information to generate a session key corresponding to the session key of said selected one of said second correspondents.

42. (new) A method according to claim 41 wherein said secret information (d) and said additional secret information (k) are combined at said selected one of said second correspondents in a signature algorithm to provide said first signature component and said additional secret information is obtained by said first correspondent by utilizing said stored secret information on said first signature component.

43. (knew) A method of claim 42 wherein said first signature component includes public information associated with said first correspondent and said first correspondent utilizes said public information to obtain said additional secret information.

44. (new) A method according to claim 42 wherein a second signature component is received by said first correspondent and is derived from said shared key.

45. (new) A method according to claim 44 wherein a portion of said shared key is utilized to provide said second signature component.

46. (new) A method according to claim 45 wherein said shared key represents the coordinates of a point on an elliptic curve and said portion is one of said coordinates.

47. (new) A method according to claim 45 wherein said portion is hashed by a secure hash function to provide said second signature component.

48. (new) A method according to claim 33 wherein said signature is verified by operating upon the session key obtained at said first correspondent to obtain a value corresponding to said second signature component and comparing such value with said second signature component.